NNH/PMD/CSG/RVC/JDG/GRV/FMZ/JSU

RESOLUCIÓN EXENTA N° 0101

MAT.: APRUEBA POLÍTICA DE USO DE LAS INTELIGENCIAS ARTIFICIALES.

SANTIAGO, 02-10-2024

VISTOS

Lo dispuesto en la Ley N° 18.989, en su Título II sobre el Fondo de Solidaridad e Inversión Social; Ley N° 20.530, que crea el Ministerio de Desarrollo Social; Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; Ley N° 18.575 de Bases Generales de Administración del Estado; Ley 21.640 de Presupuesto para el año 2024; la Resolución Nº 7/2019 que fija Normas sobre Exención del Trámite de Toma de Razón de la Contraloría General de la República; en el Decreto Supremo N° 15/2022, del Ministerio de Desarrollo Social y Familia, que nombra a persona que indica en el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social; demás antecedentes tenidos a la vista.

CONSIDERANDO

1.- Que, El Fondo de Solidaridad e Inversión Social – FOSIS, es un Servicio Público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, regulado por el Título II de la Ley 18.989, cuya misión es contribuir a la superación de la pobreza y vulnerabilidad social a través de estrategias que fortalezcan la cohesión social, las habilidades y capacidades de personas, familias y comunidades, con pertinencia territorial y enfoque de género y su finalidad es financiar en todo o en parte planes, programas, proyectos y actividades especiales de desarrollo social.

2.- Que, el Memorandum FC.MEM. 00321-2024, de fecha 11 de septiembre de 2024, enviado por doña Roxana Vercoutere Carter, encargada de Ciberseguridad del FOSIS, en el que solicita formalizar la aprobación de **POLÍTICA DE USO DE LAS INTELIGENCIAS ARTIFICIALES,** política-SSI-A-7.09, Versión 1 del 9 de septiembre de 2024.

3.- Que, El objetivo de esta política es establecer directrices claras y éticas para el desarrollo, la implementación y el uso de sistemas de IA en el Fondo de Solidaridad e Inversión Social, FOSIS.

Estas directrices están diseñadas para asegurar que la IA respete los derechos de los ciudadanos el bienestar de las personas, fomente la seguridad, confianza pública, el cumplimiento de la normativa vigente y se propenda a un desarrollo sostenible, para que sea inclusiva y globalizada.

4.- Que, en virtud del principio de formalidad que rige los actos de la Administración establecido en el artículo 3 de la Ley N° 19.880, es necesario dictar un acto administrativo aprobatorio del procedimiento referido y sus anexos.

RESUELVO

1.- APRUEBASE la Política de Uso de las Inteligencias artificiales, Política-SSI-A-7.09. Versión 1 del 9 de septiembre de 2024.

<table>
<tr><td rowspan="3">FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile</td><td rowspan="2">POLÍTICA DE USO DE LAS INTELIGENCIAS ARTIFICIALES</td><td>Fecha emisión:
09/09/2024</td></tr>
<tr><td>Versión: 1</td></tr>
<tr><td>POLÍTICA-SSI-A-7.09</td><td>Fecha versión:
09/09/2024</td></tr>
</table>

1. OBJETIVO

El objetivo de esta política es establecer directrices claras y éticas para el desarrollo, la implementación y el uso de sistemas de IA en el Fondo de Solidaridad e Inversión Social, FOSIS.

Estas directrices están diseñadas para asegurar que la IA respete los derechos de los ciudadanos el bienestar de las personas, fomente la seguridad, confianza pública, el cumplimiento de la normativa vigente y se propenda a un desarrollo sostenible, para que sea inclusiva y globalizada.

2. ALCANCE

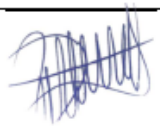
Esta política se aplica a todos los/as funcionarios/as de planta, contrata y prestadores de servicio a honorarios que tenga la necesidad de implementar o usar Inteligencias Artificiales o Aprendizaje de Maquina.

Esta Política aplica a todo usuario y usuaria que acceda, procese o almacene información del FOSIS.

Este documento aplica a todos los recursos de tecnologías de la información que se utilicen productos o servicios de analítica o apoyo de tareas basadas den Inteligencia Artificial.

Norma NCh-ISO 27001:2023 controles:

- 5.21 Gestión de riesgos: Evaluar y mitigar los riesgos asociados con el uso de sistemas de IA, incluyendo la privacidad y la seguridad de los datos procesados por estos sistemas.
- 5.23 Seguridad de los datos: Proteger la confidencialidad, integridad y disponibilidad de los datos que son utilizados por sistemas de IA. Esto incluye datos de entrenamiento, entrada y salida de los modelos de IA.
- 5.15 Acceso y control de acceso: Garantizar que solo personal autorizado tenga acceso a sistemas de IA y datos relacionados con ellos.
- 6.3 Concienciación y capacitación: Capacitar al personal en los riesgos y procedimientos de seguridad asociados a los sistemas de IA.

Elaborado por: **Roxana Vercoutere Carter** Encargada Ciberseguridad	Revisado por: **Gabriel Rosales Villarroel** Jefe Tecnologías de la Información y las telecomunicaciones	Aprobado por: **Cristian Salomó González** Encargado de Seguridad de la Información Subdirector de Usuarios
	Gabriel Fernando Rosales Villarroel Firmado digitalmente por Gabriel Fernando Rosales Villarroel Fecha: 2024.09.09 18:07:45 -03'00'	
Fecha: 09/09/2024	Fecha:	Fecha:
Documento Impreso – Copia no controlada sin timbre original		

- 8.32 Gestión de cambios: Evaluar y gestionar los cambios en los sistemas de IA y sus entornos, asegurando que la seguridad no se vea comprometida.

- 5.36 Cumplimiento legal y reglamentario: Asegurar que el uso de la IA cumpla con las leyes y regulaciones pertinentes, especialmente en lo relacionado con la protección de datos.
- 5.28 Monitoreo y revisión: Implementar procesos de monitoreo continuo y revisiones periódicas de los sistemas de IA para detectar y responder a posibles incidentes de seguridad.

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, sus políticas, procedimientos e instructivos.
- Política general de gestión de riegos FOSIS, su normativa y su plan de tratamiento anual, vigente.
- NCh-ISO 27001:2023 – Seguridad de la Información, Ciberseguridad y protección de la privacidad - Sistema de gestión de la seguridad de la información -Requisitos.
- NCh-ISO 9001:2015 – Sistema de gestión de la calidad – Requisitos
- NCh-ISO 31000:2018 - Gestión del riesgo – Directrices
- Ley N° 19.223, Tipifica figuras penales relativas a la informática.
- Ley N° 19.799, Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley 19.880, establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
- Ley N° 20.285, sobre Acceso a la Información Pública.
- Ley Nº 19.628, sobre Protección de la Vida Privada.
- Decreto Supremo N° 83/2005, del Ministerio Secretaría General de la Presidencia, que Aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Política Nacional de Inteligencia Artificial y Anexos vigentes.
- Ley 21.663/2024 Ley marco de Ciberseguridad
- Código de Ética del FOSIS, Res. Exenta FC-F-00245/10-04-2024.
- Ley 20.285, Transparencia y acceso a la información pública: en el sentido en el que el uso de las IA podría afectar aspectos de la información privada y la que se publica.
- Decreto 779, que “Aprueba reglamento del registro de bancos de datos personales a cargo de organismos públicos”: en similar sentido que la anterior.
- Ley Nº 18.834, Aprueba Estatuto Administrativo

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Comité de seguridad	- Conocer, fomentar y difundir las reglas necesarias para garantizar la seguridad de la información en el ámbito del uso de herramientas IAs.
Encargado de Seguridad de la Información Secretario técnico del Comité de seguridad de la Información	- Apoyar al Comité de Seguridad de la Información en la definición de las estrategias para garantizar la seguridad de la información en el uso de tecnologías de Inteligencia Artificial. - Validar que las protecciones definidas cumplen con las necesidades de la Institución y se encuentren ajustadas a derecho. - Monitorear las herramientas de Inteligencia Artificial adoptadas en el FOSIS para velar por el cumplimento normativo.
Jefe de Tecnologías de la Información y Telecomunicaciones	- Analizar las propuestas de uso de herramientas de Inteligencia Artificial para determinar viabilidad y pertinencia. - Analizar el ámbito de trabajo bajo la mirada de los datos que son procesados por la herramienta de Inteligencia Artificial - Monitorear el buen uso de las Inteligencias Artificiales en el ámbito del uso de los datos. - Ejecutar las solicitudes de alerta levantadas.
Subdirectores, Directores Regionales Jefes de Departamento	- Proponer y justificar el uso de herramientas de Inteligencia Artificial. - Cautelar el cumplimiento de las medidas de protección y buen uso de los datos.
Funcionarios de planta, contrata, honorarios, consultores externos y prestadores que realicen trabajos en FOSIS y para el FOSIS	- Dar cumplimiento a las directrices establecidas en la presente Política. - Reportar los incidentes de seguridad o uso ético de datos, generación de información, niveles de interpretación y análisis de datos detectados en el ámbito de las actividades de uso de las Inteligencias Artificiales. - Uso responsable y bajo el marco normativo de esta política.

5. POLÍTICA

5.1. Declaración Institucional

La Seguridad de la Información del Fondo de Solidaridad e Inversión Social, FOSIS, es el conjunto de definiciones y acciones destinadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información tanto dentro como fuera de las dependencias de la Institución, a fin de garantizar la continuidad de los procesos de la Institución y mitigar el daño que se les pudiera producir a estos activos.

El FOSIS se compromete a utilizar tecnologías de Inteligencia Artificial (IA) para mejorar la calidad de vida de los ciudadanos, promoviendo la equidad, la transparencia y la eficiencia en sus servicios. Este compromiso se basa en la creencia fundamental de que la IA debe ser utilizada de manera ética, responsable y en beneficio de toda la sociedad.

Esta Política tiene como propósito proveer los lineamientos necesarios para garantizar la seguridad y uso ético de inteligencias artificiales como producto directo o complemento de otras aplicaciones.

5.2. Definiciones y normativa vigente.

a) **Inteligencia artificial:** Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.
b) **Personas usuarias:** Personas funcionarias independiente a la calidad contractual (Planta, Contrata y Honorario)
c) **Complemento de software:** Un complemento informático, también conocido como plug-in, es una aplicación (o programa informático) que permite extender las funciones de otra aplicación.
d) **Sesgo en la IA:** Desigualdad o injusticia en los resultados de los sistemas de IA, a menudo causados por datos de entrenamiento no representativos o por decisiones de diseño que favorecen ciertos grupos sobre otros.
e) **Explicabilidad:** Capacidad de un sistema de IA para proporcionar explicaciones claras y comprensibles sobre cómo toma decisiones.
f) **Intervención Humana:** Capacidad de los humanos para supervisar, corregir o intervenir en las decisiones de los sistemas de IA.
g) **Privacidad de Datos:** Protección de la información personal de los individuos contra el acceso no autorizado y la divulgación.

5.3. Relación con las políticas y procedimientos institucionales

Esta política se aplica de forma complementaria a la normativa interna (políticas, procedimientos, instructivos, etc.) y gubernamentales definidas por el servicio, así como otros documentos pertinentes a FOSIS. Toda la documentación que forma parte del sistema de seguridad de la información se desarrolla bajo los criterios, formatos y metodologías existentes en el marco del sistema de gestión de calidad.

Especial relación se aplica con la política de gestión de la calidad, la de gestión de riesgo y la general de seguridad de la información.

5.4. Riesgos

5.4.1. Sesgo y Discriminación:

- Riesgo de que los sistemas de IA perpetúen o amplifiquen sesgos existentes en los datos o en la sociedad.

5.4.2. Privacidad y Seguridad de los Datos:

- Riesgo de comprometer la privacidad y la seguridad de los datos personales utilizados por los sistemas de IA.

5.4.3. Pérdida de Control Humano:

- Riesgo de que la dependencia excesiva de los sistemas de IA pueda llevar a una pérdida de supervisión y control humano sobre decisiones críticas.

5.4.4. Desconfianza Pública:

- Riesgo de que la falta de transparencia y explicabilidad en los sistemas de IA conduzca a una pérdida de confianza por parte del público.

5.5. Reglas de la Política

5.5.1. Trasparencia Obligatoria:

- Todos los sistemas de IA deben ser transparentes en su diseño y operación, proporcionando explicaciones claras sobre su funcionamiento y decisiones.

5.5.2. Revisión y Auditoria:

- Realizar revisiones y auditorías periódicas para asegurar que los sistemas de IA cumplen con las directrices éticas y no presentan sesgos perjudiciales.

5.5.3. Consentimiento Informado:

- Obtener el consentimiento informado de los ciudadanos antes de utilizar sus datos en sistemas de IA.
- El consentimiento siempre debe indicar la finalidad específica del uso de la información a la persona.
- Informar claramente a los ciudadanos sobre cómo se utilizarán sus datos y sus derechos en relación con el uso de la IA.

5.5.4. Seguridad de la Información:

- Implementar y mantener medidas de seguridad robustas para proteger los datos y sistemas de IA contra amenazas y vulnerabilidades.

5.5.5. Supervisión Humana:

- Asegurar que todas las decisiones críticas apoyadas por IA sean supervisadas o revisadas por humanos, especialmente en contextos sensibles o con alto impacto social.

5.6. Consideraciones Generales

5.6.1. Adaptabilidad y Evolución:

- Reconocer que esta política debe adaptarse a medida que la tecnología y el panorama regulatorio evolucionen.
- Comprometerse a revisiones periódicas y actualizaciones de la política para reflejar las mejores prácticas y los avances en la tecnología de IA.

5.6.2. Promoción de la Educación y la Conciencia:

- Fomentar la educación continua y la concienciación sobre el uso ético de la IA entre todos los funcionarios y partes interesadas del FOSIS.
- Proporcionar recursos educativos y formación para apoyar el cumplimiento de esta política.

5.6.3. Fomento de la Colaboración y el Diálogo:

- Promover la colaboración y el diálogo entre diferentes departamentos, partes interesadas y expertos en IA para asegurar una implementación y uso responsables de la IA.
- Participar en iniciativas y foros nacionales e internacionales para compartir conocimientos y experiencias en el uso de la IA.

La política pretende guiar en el uso responsable y ética de las tecnologías de inteligencia artificial, asegurando siempre el respeto a los derechos de los ciudadanos y el mejoramiento continuo de los servicios sociales y familiares.

5.6.4. Denuncias y Notificaciones

El personal del FOSIS, proveedor o tercero debe notificar toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas en el uso de inteligencias artificiales que pudiera derivar en un posible un incumplimiento, uso indebido u otra situación asociada. Se debe notificar inmediatamente al Encargado de Ciberseguridad o de acuerdo con lo establecido en el Procedimiento de Gestión de Incidentes[1].

La IA es un componente relevante en el ámbito de la ciberseguridad y ciberdefensa promoviendo sistemas tecnológicos seguro.

6. DIFUSIÓN

La comunicación de la presente política se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, mediante los siguientes canales:

- Publicación en la intranet de FOSIS
- Correo informativo.

7. SANCIONES

El incumplimiento de las obligaciones emanadas de esta política se sanciona según las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del FOSIS.

Cuando el incumplimiento se trate de personas sin responsabilidad administrativa o empresas dentro de esta política, se procede al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales derivadas de tales infracciones.

8. REVISIÓN Y MEDICIÓN

La presente política debe ser revisada a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

9. CONTROL DE VERSIONES

Versión	Fecha de Aprobación	Motivo del Cambio
1	09/09/2024	Publicación y difusión

ANOTESE, COMUNIQUESE Y PUBLIQUESE.

Nicolás Navarrete Hernández

Digitally signed by Nicolás Navarrete Hernández
Date: 2024.10.02 18:23:03 -03'00'

NICOLAS NAVARRETE HERNANDEZ

DIRECTOR EJECUTIVO

FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL.

Distribución.

Subdirección de usuarios.

Subdirección de administración y finanzas.

Oficina de Partes.